Interference in the 2.4 GHz ISM Band: Impact on the Bluetooth Access Control Performance

Nada Golmie and Frederic Mouveaux
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
Email: nada.golmie@nist.gov

Abstract— **Bluetooth is a radio technology operating in the 2.4 GHz ISM frequency band, that is emerging as a low-level and low-power wireless communication protocol used for wireless personal area networks (WPANs) where proximal devices can share information and resources. In this paper, we quantify the performance of the Bluetooth access control layer when the radio is operating in close proximity to a WLAN system. We use a probability analysis approach to derive the packet error for Bluetooth. The analytical results are validated using detailed simulation models for an interference scenario consisting of Bluetooth and WLAN devices. Packet loss is obtained for voice and data traffic for different interference conditions.**

Keywords—**WPANs, Bluetooth, Interference.**

I. Introduction

An increasingly mobile lifestyle is creating the need for Wireless Personal Area Networks (WPANs) consisting of ad-hoc communications between portable computing devices such as laptops, PDAs, pagers, and cellular telephones. What is emerging today are wireless technologies, including IEEE 802.11 [1], and Bluetooth [2], that promise to outfit portable and embedded devices with high bandwidth, localized wireless communication capabilities that can also reach the globally wired Internet.

Due to its almost global availability, the 2.4 GHz Industry Scientific and Medical (ISM) unlicensed band constitutes a popular frequency band suitable to low cost radios. New proposed solutions for WPANs such as IEEE 802.15 and Bluetooth plan to operate in the 2.4 GHz ISM band while IEEE 802.11 [1] has standards for Wireless Local Area Networks operating in this band and microwave ovens are a primary user of the band at 2.45 GHz. Therefore, it is anticipated that some interference will result from all these technologies operating in the same environment and frequency space. Furthermore, since IEEE 802.11, and Bluetooth devices may likely come together in a laptop or may be close together at a desktop, interference may lead to significant performance degradation.

The main goal of this paper is to present our results on the performance of a Bluetooth access control system when its radio is operating in close proximity to an IEEE 802.11 system. The evaluation of interference in the 2.4 GHz band has been receiving more attention lately. Zurbes et. al. simulate the impact of 100 co-located sessions on the Bluetooth radio performance [3]. Kamerman reports on tolerable interference levels between Bluetooth and 802.11 devices for various scenarios and device positions [4]. His analysis is based on a simple path loss model and Signal to Interference (SIR) requirements for Bluetooth and 802.11 receivers. Furthermore, the probability of an 802.11 packet error in the presence of a Bluetooth piconet has been derived by Ennis [5], then extended by Shellhammer [6] and Chiasserini and Rao [7].

In this paper, we first use a probability analysis approach to capture the interference environment. Our analytical results are then validated against simulation results obtained from detailed simulation models of the Bluetooth and IEEE 802.11 Medium Access Control (MAC) and Physical (PHY) layers. Our goal is to give additional insights on the performance of Bluetooth voice and data traffic under different interference traffic conditions.

This paper is organized as follows. In sections II and III we give some general insights on the Bluetooth and IEEE 802.11 protocol operation respectively. In section IV, we present our interference analysis and the probability that a packet containing error is received at the Bluetooth node. In section V, we evaluate the impact of WLAN interference on the Bluetooth performance and present simulation results. Concluding remarks are offered in section VI.

II. Bluetooth Protocol Overview

In this section, we give a brief overview of the Bluetooth technology [2] and discuss the main functionality of its protocol specifications which consist of several modules, namely, the Radio Frequency (RF), Baseband (BB) and Link Manager (LM). Bluetooth is a short range (0 m - 10 m) wireless link technology aimed at replacing non-interoperable proprietary cables that connect phones, laptops, PDAs and other portable devices together. Bluetooth operates in the ISM frequency band starting at 2.402 GHz and ending at 2.483 GHz in the USA, and Europe. 79 RF channels of 1 MHz width are defined. The air interface is based on an antenna power of 1 mW (0 dBi gain). The signal is modulated using binary Gaussian Frequency Shift Keying (GFSK). The raw data rate is defined at 1 Mbits/s. A Time Division Multiplexing (TDM) technique divides the channel into 625 μs slots. Transmission occurs in packets that occupy an odd number of slots (up to 5). Each packet is transmitted on a different hop frequency with a maximum frequency hopping rate of 1600 hops/s.

Two or more units communicating on the same channel form a piconet, where one unit operates as a master and the others (a maximum of seven active at the same time) act as slaves. A channel is defined as a unique pseudo-random frequency hopping sequence derived from the master device's 48-bit address and its Bluetooth clock value. Slaves in the piconet synchronize their timing and frequency hopping to the master upon connection establishment. In the connection mode, the master controls the access to the channel using a polling scheme where master and slave transmissions alternate. A slave packet always follows a master packet transmission as illustrated in Figure 1 that depicts the master's view of the slotted TX/RX channel.

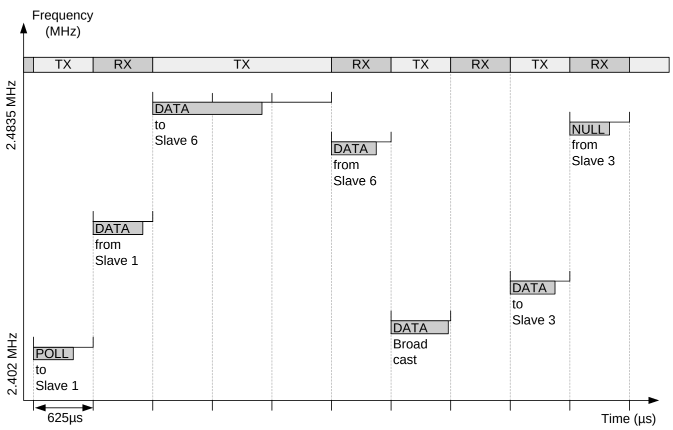

Fig. 1. Master TX/RX Hopping Sequence

There are two types of link connections that can be established between a master and a slave: the Synchronous Connection-Oriented (SCO), and the Asynchronous Connection-Less (ACL) link. The SCO link is a symmetric point-to-point connection between a master and a slave where the master sends an SCO packet in one TX slot at regular time intervals, defined by T_{SCO} time slots. The slave responds with an SCO packet in the next TX opportunity. T_{SCO} is set to either 2, 4 or 6 time slots for $HV1$, $HV2$, or $HV3$ packet formats respectively. All three formats of SCO packets are defined to carry 64 Kbits/s of voice traffic and are never retransmitted in case of packet loss or error. The ACL link, is an asymmetric point-to-point connection between a master and active slaves in the piconet. Several packet formats are defined for ACL, namely $DM1$, $DM2$, and $DM3$ packets that occupy 1, 3, and 5 time slots respectively. An Automatic Repeat Request (ARQ) procedure is applied to ACL packets where packets are retransmitted in case of loss until a positive acknowledgement (ACK) is received at the source. The ACK is piggy-backed in the header of the returned packet where an ARQN bit is set to either 1 or 0 depending on whether the previous packet was successfully received or not. In addition, a sequence number (SEQN) bit is used in the packet header in order to provide a sequential ordering of data packets in a stream and filter out retransmissions at the destination. Forward Error Correction (FEC) is used on some SCO and ACL packets in order to correct errors and reduce the number of ACL retransmissions.

III. IEEE 802.11 Protocol Overview

The IEEE 802.11 standard [1] defines both the physical (PHY) and medium access control (MAC) layer protocols for WLANs. In this sequel, we will be using WLAN and 802.11 interchangeably.

The IEEE 802.11 standard calls for three different PHY specifications: frequency hopping (FH) spread spectrum, direct sequence (DS) spread spectrum and infrared (IR). The transmit power for DS and FH devices is defined at a maximum of 1 W and the receiver sensitivity is set to -80 dBm. Antenna gain is limited to 6 dBi maximum.

Under FH, each station's signal hops from one modulating frequency to another in a predetermined pseudo-random sequence. Both transmitting and receiving stations are synchronized and follow the same frequency sequence. There are 79 channels defined in the (2.4000 - 2.4835) GHz region spaced 1 MHz apart. The time each radio dwells on each frequency depends on each individual implementation and government regulation. The basic access rates of 1 and 2 Mbits/s use multilevel Gaussian frequency shift keying (GFSK).

A DS transmitter converts the data stream into a symbol stream where each symbol represents a group of multiple bits to spread over a relatively wideband channel of 22 MHz. The basic data rate is 1 Mbits/s encoded with differential binary phase shift keying (DBPSK) or 2 Mbits/s using differential quadrature phase shift keying (DQPSK). Higher rates of 5.5 and 11 Mbits/s are also available with techniques combining pulse-position-modulation (PPM) and quadrature amplitude modulation (QAM).

The IEEE 802.11 MAC layer specifications common to all PHYs and data rates coordinate the communication between stations and control the behavior of users who want to access the network. The Distributed Coordination Function (DCF) which describes the default MAC protocol operation is based on a scheme known as carrier-sense, multiple access, collision avoidance (CSMA/CA). Both the MAC and PHY layers cooperate in order to implement collision avoidance procedures. The PHY layer samples the received energy over the medium transmitting data and uses a clear channel assessment (CCA) algorithm to determine if the channel is clear. This is accomplished by measuring the RF energy at the antenna and determining the strength of the received signal commonly known as RSSI, or received signal strength indicator. In addition, carrier sense can be used to determine if the channel is available. This technique is more selective since it verifies that the signal is the same carrier type as 802.11 transmitters. A virtual carrier sense mechanism is also provided at the MAC layer. It uses the request-to-send (RTS) and clear-to-send (CTS) message exchange to make predictions of future traffic on the medium and updates the network allocation vector (NAV) available in stations. Communication is established when one of the wireless nodes sends a short RTS frame. The receiving station issues a CTS frame that echoes the senders address. If the CTS frame is not received, it is assumed that a collision occurred and the RTS process starts over. Regardless of whether the virtual carrier sense routine is used or not, the MAC is required to implement a basic access procedure (depicted in Figure 2) as follows. If a station has data to send, it waits for the channel to be idle through the use of the CSMA/CA algorithm. If the medium is sensed idle for a period greater than a DCF interframe space (DIFS), the station goes into a backoff procedure before it sends its frame. Upon the successful reception of a frame, the destination station returns an ACK frame after a Short interframe space (SIFS). The backoff window is based on a random value uniformly distributed in the interval $[0, CW]$

where CW represents the Contention Window parameter and is varied between CW_{min} and CW_{max}. If the medium is determined busy at any time during the backoff slot, the backoff procedure is suspended. It is resumed after the medium has been idle for the duration of the DIFS period. If an ACK is not received within an ACK timeout interval, the station assumes that either the data frame or the ACK was lost and needs to retransmit its data frame by repeating the basic access procedure.

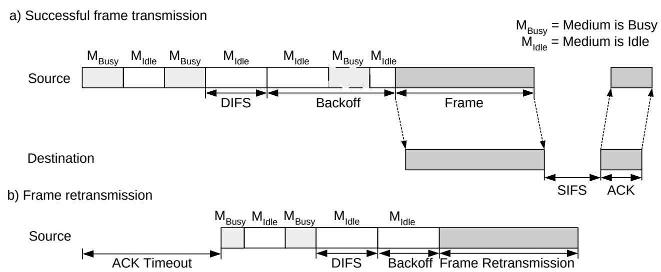

Fig. 2. WLAN Frame Transmission Scheme

IV. INTERFERENCE ANALYSIS

Since we are mainly concerned with evaluating the Bluetooth performance in an interference environment, we consider a Bluetooth receiver node as our reference and derive the probability that a packet containing errors (at least one error), P(PE), is received at this node. The interfering signal is assumed to be from proximally located WLAN devices.

A collision occurs when both the Bluetooth and the interfering packets overlap in time and frequency. This collision is detected at the Bluetooth receiver in the form of SIR that depends on the power transmitted, the distance traveled, and the path loss model used. The SIR then translates into a Bit Error Rate (BER) according to the GFSK carrier modulation and the Bluetooth receiver implementation used.

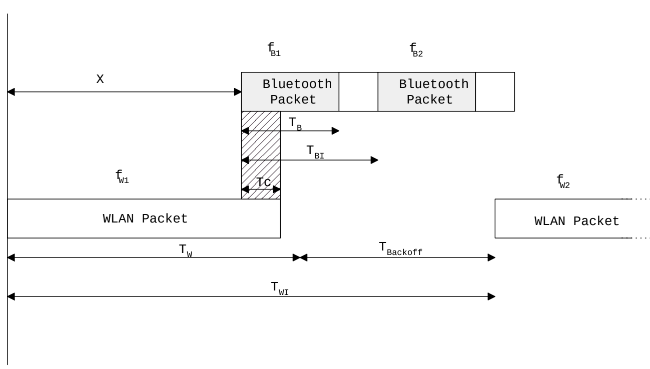

Fig. 3. Collisions at the Bluetooth Receiver Node

Figure 3 illustrates the timing of the Bluetooth packets with respect to WLAN packets. Let f_B and f_W be the frequencies used to transmit the Bluetooth and WLAN packets respectively. We denote by T_B and T_W, the Bluetooth and the WLAN packet transmission periods respectively. In order to determine the position of the Bluetooth packet with respect to the WLAN packet when both systems use the same frequency ($f_B = f_W$), we define a variable X that represent the time offset between a Bluetooth and a WLAN packet. Let T_C represent the time interval when both WLAN and Bluetooth packets overlap. We denote by T_{WI} the interval between two WLAN packets including the packet transmission time T_W and a backoff period, $T_{Backoff}$. $T_{Backoff}$ is the sum of several variables such as SIFS, DIFS, the ACK transmission time, and C_W. Similarly, we denote by T_{BI}, the interval between two Bluetooth packet transmissions. Due to the slotted structure of the Bluetooth channel, a packet transmission occurs at the boundary of a Bluetooth time slot. We assume that X is a random variable that is uniformly distributed between zero and T_{WI}. Note that X is a continuous random variable, however in this analysis it is quantified to the resolution of a Bluetooth symbol period at the rate of a symbol (or a bit) per μs.

$$X \sim U(0, T_{WI}) \tag{1}$$

Thus, the probability that a Bluetooth packet overlaps in time and frequency with a WLAN packet depends on:

- The position of the WLAN packet with respect to the Bluetooth packet, i.e. X
- The transmission frequencies, f_B and f_W of the Bluetooth and WLAN systems respectively

The probability mass function of X is equal to $p_X(k) = \frac{1}{T_{WI}}$ where $k = 1, 2, ..T_{WI}$. Both the Bluetooth and WLAN systems have a frequency hopping span of 79 channels. The probability that a WLAN system lands on the same frequency as a Bluetooth system depends on a discrete random variable f_W whose probability mass function is $p_{f_W}(j) = \frac{n}{79}$ where j varies between 1 and 79 and n determines the number of overlapping channels. For FH $n = 1$, while for DS WLAN systems, $n = 22$.

Expressing $P(PE)$ as a joint probability of frequency and packet overlap yields:

$$P(PE) = \sum_{k=0}^{T_{WI}} P(PE \mid X = k; f_W = j) p_X(k) p_{f_W}(j)$$

where $P(PE \mid X = k; f_W = j)$ depends on T_C and BER. Thus, we write:

$$P(PE \mid X = k; f_W = j) = 1 - (1 - BER)^{T_C} \tag{2}$$

Therefore,

$$P(PE) = (\frac{n}{79})(\frac{1}{T_{WI}}) \sum_{k=0}^{T_{WI}} (1 - (1 - BER)^{T_C}) \tag{3}$$

The value of T_C depends on X, T_W, and T_B. We distinguish three cases.

- $T_B \leq T_W$ and $T_B \leq T_{WI}$-T_W

$$T_C = \begin{cases} T_B & \text{if } X \leq T_W - T_B \\ T_W - X & \text{if } T_W - T_B < X < T_W \\ 0 & \text{if } T_W \leq X \leq T_{WI} - T_B \\ X + T_B - T_{WI} & \text{if } T_{WI} - T_B < X \leq T_{WI} \end{cases} \tag{4}$$

- $T_B \leq T_W$ and $T_B > T_{WI}$-T_W

$$T_C = \begin{cases} T_B & \text{if } X < T_W - T_B \\ T_W - X & \text{if } T_W - T_B \leq X < T_{WI} - T_B \\ T_W + T_B - T_{WI} & \text{if } T_{WI} - T_B \leq X \leq T_W \\ X + T_B - T_{WI} & \text{if } T_W < X \leq T_{WI} \end{cases} \tag{5}$$

- $T_B > T_W$;
  We let $N(X)$ be the number of WLAN packets that hit a Bluetooth packet.

$$N(X) = \begin{cases} \lceil \frac{T_B}{T_{WI}} \rceil & \text{if } X \leq T_{WI} \lceil \frac{T_B}{T_{WI}} \rceil - T_B \\ \lceil \frac{T_B}{T_{WI}} \rceil + 1 & \text{otherwise} \end{cases} \tag{6}$$

We also define T_i as the interval of time overlap with WLAN packet i.

$$T_i = \begin{cases} max(T_W - X, 0) & \text{if } i = 1 \\ T_W & \text{if } i = 2, .., N(X) - 1 \\ min(X + T_B - (N(X) - 1) \times T_{WI}, T_W) & \text{if } i = N(X) \end{cases} \tag{7}$$

In this case T_C is basically the sum of all T_i's over $N(X)$ colliding WLAN packets.

$$T_C = \sum_{i=1}^{N(X)} T_i \tag{8}$$

V. Simulation Results

Our goal in this section is to validate the analytical interference model presented in section IV. We used *OPNET*[1] to develop a simulation model for the Bluetooth protocol. We partially implement the Baseband and L2CAP layer according to the specifications [2] and use the configuration and system parameters shown in Table I. We assume that a connection is already established between the master and the slave and that the synchronization process is complete. The connection type is either SCO for voice or ACL for data traffic. For WLAN we use the models provided by the OPNET modeler's library.

For the Bluetooth signal we assume a pair of devices; a master and a slave device located at (0,0) and (1,0) meters respectively. Master and slave devices are transmitting either voice or data traffic. For voice traffic, we consider a symmetric stream of 64 kbits/s each way. We use $HV1$ packets that have a total size of 366 bits including a header and an access code of 126 bits. $HV1$ packets are sent every $T_{SCO} = 2$ or 1250 μs. $HV1$ payload bits are corrected with a 1/3 FEC rate.Since the payload does not have a CRC, errors in the payload do not yield

[1]OPNET is a trademark of OPNET Technologies Inc.

TABLE I

Simulation Parameters

System Parameters	**Values**
Propagation delay	5 μs/km
Length of simulation run	30 seconds
Length of run prior to gathering statistics	10 % of simulated time
Bluetooth Parameters	**Values**
Data Rate	1 Mbits/s
ACL Baseband Packet Encapsulation	DM5
SCO Baseband Packet Encapsulation	HV1
Number of Devices	2 (1 Master, 1 Slave)
Master Coordinates	(1,0) (meters)
Slave Coordinates	(0,0) (meters)
Transmitted Power	1 mW
WLAN Parameters	
Packet Interarrival Time for 1 Mbits/s	10.56 ms
Packet Interarrival Time for 11 Mbits/s	2.52 ms
Transmitted Power	1 mW
Source Coordinates	(0,0.15) (meters)
Sink Coordinates	(0,10) (meters)
Packet Header	224 bits
T_W	includes Packet Header
T_{WI}	includes Backoff and T_W
Slot Time	$2 * 10^{-5}$ seconds
SIFS Time	$1 * 10^{-5}$ seconds
DIFS Time	$5 * 10^{-5}$ seconds
CW_{min}	31
CW_{max}	1023
Fragmentation Threshold	None
RTS Threshold	None
Short Retry Limit	4
Long Retry Limit	7

to dropping packets. In addition, a 1/3 FEC rate is applied to the header and a Hamming code ($d = 14$) is applied to the access code. Uncorrected errors in either the header or the access code lead to dropping packets. For the data traffic, we consider a LAN access application. Both master and slave devices generate $DM5$ type packets every 0.01250 seconds, thus utilizing 50% of the 1 Mbits/s channel. $DM5$ packets have a total size of 2871 bits, including a 54-bit header and a 72-bit access code and occupy 5 Bluetooth slots. A 2/3 FEC rate is used to correct payload errors, while errors in the header or access code are corrected with a 1/3 FEC and a Hamming code ($d = 14$) respectively. Uncorrected errors in either the packet header or payload lead to dropping packets.

For the WLAN signal, we use two 802.11 Direct Sequence devices transmitting at 1 Mbits/s. We assume unidirectional traffic; a WLAN source transmits packets to a WLAN sink that returns ACK messages to the source. The WLAN source and sink devices are located at (0,0.15) and (0,10) meters respectively. Traffic sent from the WLAN source constitute the interference signal to the Bluetooth slave device.

We present the results from two different simulation experiments that show the impact of interference on Bluetooth devices for different applications, namely voice and data traffic.

Experiment 1- We vary the WLAN packet length, T_W, and the interarrival packet, T_{WI}, while keeping the WLAN offered load fixed at 50% of the 1 Mbits/s channel capacity. Thus, T_W and T_{WI} are varied from 500 and 1000 μs to 8000 and 16000 μs respectively. Note that T_B and T_W denote the packet length in time and are also equivalent to the packet size in bits assuming a data rate of 1 MBits/s.

Experiment 2- We fix T_W at 1000 μs and vary T_{WI} according to $\frac{T_W}{OL}$ where OL is the offered load as a percentage of the 1 Mbits/s channel capacity.

Table II summarizes the experiments.

TABLE II
VALIDATION EXPERIMENT SUMMARY

Experiment	WLAN Offered Load	WLAN Traffic
Experiment 1	50% of Channel Capacity	T_W and T_{WI} variable
Experiment 2	Variable	$T_W = 1000\ \mu$s, $T_{WI} = \frac{T_W}{OL}$

Given that the WLAN source is at a distance, $d_I = 0.15$m from the Bluetooth slave, while the Bluetooth master is at a distance, $d_M = 1$m, and assuming that both the WLAN source and the Bluetooth master device transmit at 1mW, the SIR at the slave is given by $20log\frac{d_I}{d_M} \approx -16$ dB [2]. The choice of the BER value corresponding to this SIR is based on the PHY results of the Bluetooth receiver used [8]. We note that when the Signal-to-noise ratio (SNR) is above 25 dB and the SIR is below -10 dB, the BER is ~ 0.3 for Bluetooth frequency offsets of 10 MHz from the WLAN DS center frequency. Therefore, we use $BER = 0.3$ and $n = 10$ in our analysis. A summary of the parameters used in the analysis is provided in Table III.

TABLE III
ANALYSIS PARAMETERS

Parameters	Values
T_B	366 for $HV1$ and 2871 for $DM5$
T_W and T_{WI}	Variable
n	20
BER	0.3

All simulations are run for 1000 seconds of simulated time and the first 10 % of the data is discarded. The performance measurements are logged at the slave device. The metric we use includes the packet loss, P_L, and the packet error, P_E. The packet loss is the number of packets discarded due to uncorrected errors in the packet divided by the total number of packets transmitted. While the packet error is the number of packets received with at least one error (prior to applying error correction on the packet and deciding whether to keep it or drop it). Note that Equation 3 captures the probability that a packet containing at least one error is received at the Bluetooth node. Since different error correcting schemes are applied on different packet types and packet segments, this corresponds to the packet error metric rather than the packet loss.

The simulation model used for this validation assumes the following:

- The WLAN CCA is limited to carrier sense functionality capable of detecting other WLAN devices of the same kind (either FH or DS) but cannot detect the presence of Bluetooth devices.
- The impact of Bluetooth interference on WLAN is disabled in order not to change the WLAN traffic distribution. That is interference from Bluetooth does not cause errors at the WLAN receiver.

[2] Assuming the logarithmic path loss model given in [4]

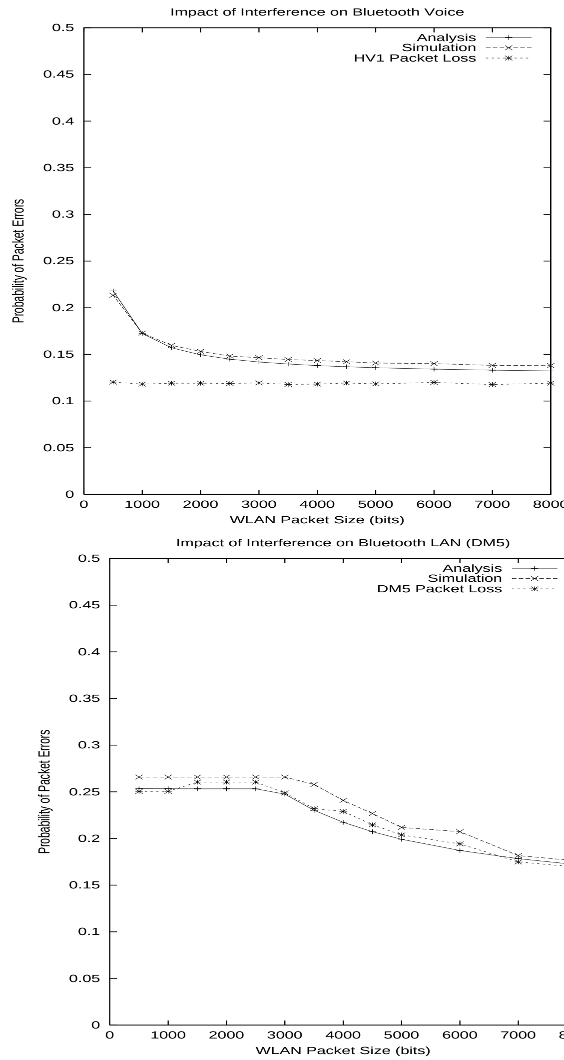

Fig. 4. $\boxed{\frac{(a)}{(b)}}$ Varying T_W and T_{WI} for a 50% WLAN Offered Load (a) Impact of WLAN Interference on Bluetooth Voice (b) Impact of WLAN Interference on Bluetooth LAN

- The BER value used in the Bluetooth receiver is computed according to the receiver's DSP model and varies according to the frequency hop and the signal to interference ratio.

Figure 4 (a) gives the probability of packet error for the Bluetooth voice traffic for different WLAN packet lengths. We note that the analytical results closely approximate the simulation results. The probability of packet error varies between $\sim$ (22% - 13%), while the probability of packet loss remains at $\sim$ 12%. As expected, the packet loss is lower than the packet error due to the use of different error correction schemes applied on different segments of the packet. We note that errors occurring in the payload of $HV1$ packets do not lead to dropping packets. Furthermore, if errors in the header can be corrected the packet is kept, otherwise the packet is dropped. This explains the difference between the packet loss and the packet error.

A similar trend applies to the Bluetooth LAN results given in Figure 4(b). The packet error varies between $\sim$ (25% - 17%). The difference between the packet loss and the packet error is not as significant as in Experiment 1 (a). In fact, the decision to drop $DM5$ packets is based on uncorrected errors in either the header or the payload. Therefore, the packet loss and packet error measures are very close.

Figure 5(a) and (b) illustrate the effect of varying the WLAN offered load on the Bluetooth voice and LAN performance respectively. The probability of voice packet error and packet loss increase proportionally to the WLAN offered load (Figure 5 (a)). We also note that the difference between the packet error and the packet loss is significant (∼10%) at high WLAN offered loads (65%). Note that only packet header collisions affect the packet loss. As more interfering packets are transmitted (increase in WLAN offered load), only a small number of them will ”hit” the header and cause a collision.

The results for the Bluetooth LAN are given in Figure 5(b)). The increase in packet error levels off at ∼ 25% for WLAN offered loads greater than 25%. This ”threshold” phenomenon is a direct effect of having reached an error threshold number per packet. Additional errors above that threshold do not yield to more packets being dropped.

VI. Concluding Remarks

We presented results on the performance of Bluetooth in the presence of WLAN interference based on a probability of packet collision in frequency and time overlap at the Bluetooth receiver. We first observe that the probability of packet error analysis, in the tractable case where mutual interference effects are not considered and only a particular receiver is studied, can provide a close approximation to the packet error and the packet loss measures. Furthermore, the results clearly show that packet loss due to interference may be significant (up to 27% for data traffic and 25% for voice applications) and may lead to severe performance degradation. In addition, longer Bluetooth packets (such as $DM5$ packets) are more prone to packet loss than shorter packets ($HV1$). Note that, although the packet loss is lower than the packet error for voice traffic, the quality of the audio channel is likely to be impaired due to the high number of residual errors in the payload.

More generally, the experiments stress the importance of defining accurate traffic models and distributions in the evaluation of interference. Both the offered load and the packet length are necessary parameters in order to completely specify the interference signal.

Our future work includes investigating simulation scenarios where both WLAN and Bluetooth interference can be studied together. This may unravel various intricate effects about the traffic distribution and the overall system performance of Bluetooth and WLAN operating in the 2.4 GHz frequency band.

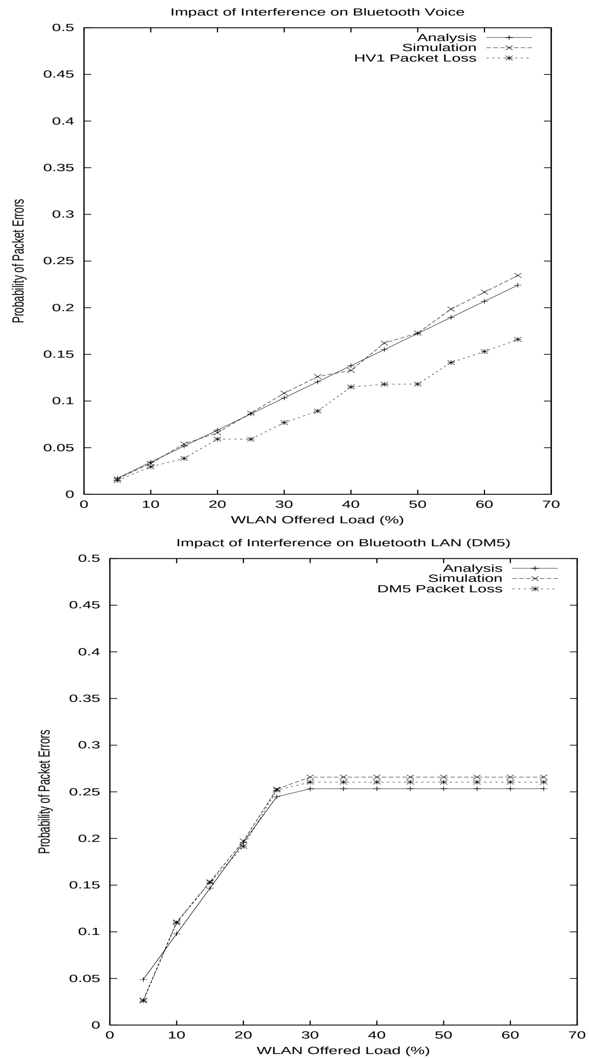

Fig. 5. $\boxed{\frac{(a)}{(b)}}$ Varying WLAN Offered Load (T_W =1000 bits) (a) Impact of WLAN Interference on Bluetooth Voice (b) Impact of WLAN Interference on Bluetooth LAN

References

[1] IEEE Std. 802-11, “IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification ,” June 1997.

[2] Bluetooth Special Interest Group, “Specifications of the Bluetooth System, vol. 1, v.1.0B ’Core’ and vol. 2 v1.0B ’Profiles’,” December 1999.

[3] S. Zurbes, W. Stahl, K. Matheus, and J. Haartsen, “Radio network performance of bluetooth ,” in *Proceedings of IEEE International Conference on Communications, ICC 2000*, New Orleans, LA, June 2000, vol. 3, pp. 1563–1567.

[4] A. Kamerman, “Coexistence between Bluetooth and IEEE 802.11 CCK: Solutions to avoid mutual interference,” in *IEEE P802.11 Working Group Contribution, IEEE P802.11-00/162r0*, July 2000.

[5] G. Ennis, “Impact of Bluetooth on 802.11 Direct Sequence,” in *IEEE P802.11 Working Group Contribution, IEEE P802.11-98/319*, September 1998.

[6] S. Shellhammer, “Packet Error Rate of an IEEE 802.11 WLAN in the Presence of Bluetooth,” in *IEEE P802.15 Working Group Contribution, IEEE P802.15-00/133r0*, Seattle, Washington, May 2000.

[7] C.F. Chiasserini, R. Rao, “Performance of IEEE 802.11 WLANs in a Bluetooth Environment,” in *IEEE Wireless Communications and Networking Conference, WCNC 2000*, Chicago, IL, September 2000.

[8] A. Soltanian and R. E. Van Dyck, “Physical layer performance for coexistence of Bluetooth and IEEE 802.11b,” in *to appear in Virginia Tech Symposium on Wireless Personal Communications*, June 2001.